CYBER SECURITY

+$92.6 million in Program Increases

FY 2014 Overview

Cyber crimes are becoming more common, more sophisticated, and more dangerous. Our adversaries increasingly use computers and the Internet to further their illicit activities. Terrorists seek to sabotage critical infrastructure; organized crime syndicates seek to defraud banks and corporations; and spies seek to steal defense and intelligence secrets and intellectual property. Each threatens our Nation's economy and security.

The Department has a unique and critical role in cyber security that emphasizes domestic mitigation of threat actors and involves countering the threat by investigating and prosecuting intrusion cases, gathering intelligence in support of nation state attribution, and providing legal and policy support to other departments. The Department is also responsible for establishing effective internal network defense and serving as a model for other departments and agencies.

The Department is committed to carrying out its role consistent with the Administration's Executive Order on Improving Critical Infrastructure Cyber Security, which emphasizes intelligence and information sharing as well as the preservation of privacy, data confidentiality, and civil liberties. One of the most important aspects of the Executive Order is its emphasis on improving government mechanisms for providing timely cyber threat information to the private sector so it may better protect and defend itself against cyber threats. Under the Executive Order, each federal department and agency is also required to develop and implement privacy and civil liberties safeguards in concert with its cyber security activities.

The Department's FY 2014 Budget provides a total of $668 million in cyber resources to address computer intrusions and cybercrimes and defend the security of the Department's critical information networks. This request includes an increase of $92.6 million to support efforts to combat and keep pace with increasingly sophisticated and rapidly evolving cyber threats. For the FBI, the budget includes an increase of $86.6 million to support the FBI's Next Generation Cyber Initiative, which will more strategically focus the FBI's efforts on the greatest cyber threat — intrusions into government and industry computer networks.   Resources are provided to enhance the technical capabilities of FBI investigative personnel, increase cyber investigations, and improve cyber collection and analysis.

For the National Security and Criminal Divisions, the budget includes an increase of $6.1 million to bolster prosecutorial efforts, strengthen policy development and legal oversight (including advice to investigative agencies and to agencies conducting network defense activities that implicate surveillance statutes), and enhance international cooperation and outreach.

Lastly, the Department continues to maintain and strengthen its own cyber security environment to counter cyber threats, including insider threats, and to ensure its personnel have unimpeded access to the IT systems, networks, and data necessary to achieve their missions. The Department has made significant investments to implement sound network security best practices and technology. Our work in this area prepares us to fulfill our cyber security responsibilities during a cyber event and establishes the Department as a model of effective and efficient network defense.

Program Increases

Federal Bureau of Investigation (FBI)
- **Next Generation Cyber : $86.6 million and 152 positions (60 agents)**

  The requested funding will support the Next Generation Cyber Initiative and will increase cyber investigation capabilities and victim identification by adding 50 special agents and 50 computer scientists; improve cyber collection and analysis; and extend centralized analytical capabilities to the field by deploying cyber workstations to serve as portals for communication intrusion-related data bureau-wide.FY2014 current services for this initiative are 1,333 positions(756 agents) and $314.0 million

National Security Division (NSD)
- **Combating Cyber Threats to National Security: $3.5 million and 26 position attorneys)**

  This increase will enable NSD to strengthen its investigative, prosecutorial, intelligence collection, and oversight abilities to support the Intelligence Community in identifying and disrupting cyber threats to national security.FY 2014 current services for this program are 138 positions(132 attorneys) and $27.0 million

Criminal Division (CRM)
- **Cyber Security: $2.6 million and 25 positions (9 attorneys)**

  This request will enable CRM to combat the growing and evolving cyber threat. As the skill and organization of technologically sophisticated transnational criminals continues to increase, the Division will require additional resources to meet these new challenges. This enhancement will increase the Division's capability in four key areas: cybercrime investigations and prosecutions; advice and advocating legal tools and authorities; international cooperation and outreach; and forensic support. This increased capacity will allow the Division to successfully deter, investigate, and punish the theft of sensitive electronic information and other cybercrime.FY 2014 current servicesfor this initiative are 122 positions (79 attorneys) and $27.9million.

FY 2014 Program Increase Summary
(Amount in $000s)

Component/Initiative	Positions	Agents	Attorneys	Amount
Federal Bureau of Investigation	**152**	**60**	**0**	**$ 86,584**
Next Generation Cyber	152	60	0	86,584
National Security Division	**26**	**0**	**16**	**$ 3,468**
Combatting Cyber Threats to National Security	26	0	16	3,468
Criminal Division	**25**	**0**	**9**	**$ 2,580**
Cyber Security	25	0	9	2,580
Grand Total, Program Increases	**203**	**60**	**25**	**$ 92,632**